

1 WE CLAIM

2

- 3 1. A method of authenticating a pair of correspondents A,B to permit
4 exchange of information therebetween, each of said correspondents having a
5 respective private key a,b and a public key p_A,p_B derived from a generator α and
6 respective ones of said private keys a,b , said method including the steps of
7 i) a first of said correspondents A selecting a first random integer x and
8 exponentiating a function $f(\alpha)$ including said generator to a power $g^{(x)}$ to provide a
9 first exponentiated function $f(\alpha)^{g^{(x)}}$;
10 ii) said first correspondent A forwarding to a second correspondent B a message
11 including said first exponentiated function $f(\alpha)^{g^{(x)}}$;
12 iii) said correspondent B selecting a second random integer y and exponentiating a
13 function $f(\alpha)$ including said generator to a power $g^{(y)}$ to provide a second
14 exponentiated function $f(\alpha)^{g^{(y)}}$;
15 iv) said second correspondent B constructing a session key K from information
16 made public by said first correspondent A and information that is private to said
17 second correspondent B, said session key K also being constructible by said first
18 correspondent A for information made public by B and information that is private to
19 said first correspondent A;
20 v) said second correspondent B generating a value h of a function $F[\delta,K]$
21 where $F[\delta,K]$ denotes a cryptographic function applied conjointly to δ and K and
22 where δ is a subset of the public information provided by B thereby to bind the values
23 of δ and K ;
24 vi) said second of said correspondents B forwarding a message to said first
25 correspondent A including said second exponential function $f(\alpha)^{g^{(y)}}$ and said value h
26 of said cryptographic function $F[\delta,K]$;
27 vii) said first correspondent receiving said message and computing a session key
28 K' from information made public by said second correspondent B and private to said
29 first correspondent A;
30 viii) said first correspondent A computing a value h' of a cryptographic function

1 $F[\delta, K']$; and

2 ix) comparing said values obtained from said cryptographic functions F to
3 confirm their correspondence.

4

5 2. A method of claim 1 wherein said message forwarded by said first
6 correspondent includes an identification of the first correspondent.

7

8 3. A method according to claim 1 wherein said message forwarded by
9 said second correspondent includes an identification of said second correspondent.

10

11 4. A method according to claim 3 wherein said message forwarded by
12 said first correspondent includes an identification of the first correspondent.

13

14 5. A method according to claim 1 wherein said first function $f(\alpha)$
15 including said generator is said generator itself.

16

17 6. A method according to claim 1 wherein said second function $f(\alpha)$
18 including said generator is said generator itself.

19

20 7. A method according to claim 6 wherein said first function $f(\alpha)$
21 including said generator is said generator itself.

22

23 8. A method according to claim 1 wherein said first function including
24 said generator $f(\alpha)$ includes said public key p_B of said second correspondent.

25

26 9. A method according to claim 1 wherein said second function including
27 said generator $f\alpha$ includes said public key p_A of said first correspondent.

28

29 10. A method according to claim 1 wherein said cryptographic functions F
30 are hashes of δ and K .

- 1
- 2 11. A method of transporting a key between a pair of correspondents A,B
- 3 to permit exchange of information therebetween, each of said correspondents having a
- 4 respective private key a, b and a public key p_A, p_B derived from a generator α and
- 5 respective ones of said private keys a, b , said method including the steps of
- 6 i) a first of said correspondents A selecting a first random integer x and
- 7 exponentiating a function $f(\alpha)$ including said generator to a power $g^{(x)}$ to provide a
- 8 first exponentiated function $f(\alpha)^{g^{(x)}}$;
- 9 ii) said first correspondent A forwarding to a second correspondent B a message
- 10 including said first exponentiated function $f(\alpha)^{g^{(x)}}$;
- 11 iii) said second correspondent B constructing a session key K from information
- 12 made public by said first correspondent A and information that is private to said
- 13 second correspondent B, said session key K also being constructible by said first
- 14 correspondent A from information made public by B and information that is private to
- 15 said first correspondent A;
- 16 iv) both of said first correspondent A and said second correspondents B
- 17 computing a respective value h, h' of function $F[\delta, K]$ where $F[\delta, K]$ denotes a
- 18 cryptographic function applied to δ and K and where δ is a subset of the public
- 19 information provided by one of said correspondents;
- 20 v) at least one of said correspondents comparing said values h, h' obtained from
- 21 said cryptographic function F to confirm their correspondence;
- 22
- 23 12. A method of claim 11 wherein said message forwarded by said first
- 24 correspondent includes an identification of the first correspondent.
- 25
- 26 13. A method according to claim 11 wherein said message forwarded by
- 27 said first correspondent includes said value obtained from said cryptographic function
- 28 by said first correspondent.
- 29
- 30 14. A method according to claim 11 wherein said values obtained from

1 said cryptographic functions are obtained from a hash of said public information and
2 said session key K.

3

4 15. A method according to claim 11 wherein said first correspondent
5 selects a pair of random integers x and t and generates a session key K as $f(\alpha)^{g(t)}$, and
6 generates a value r from said first exponentiated function $f(\alpha)^{g(x)}$ which includes a
7 factor exponentiating said public key p_B of said second correspondent B with said
8 random integer t to be of the form $p_B^{E(t)\alpha^{g(x)}}$.

9

10 16. A method according to claim 15 wherein said first correspondent A
11 generates a value s from a combination of said random integer x and said private key a
12 and forwards said value of r and said value of s to said second correspondent B to
13 permit said second correspondent B to recover said session key K using the private
14 key b of said second correspondent B.

15

16 17. A method according to claim 16 wherein said random integer x and
17 said private key a are combined to produce s such that $s = x - ra \bmod (p-1)$.

18

19 18. A method according to claim 17 wherein said cryptographic function F
20 is a hash of said public information δ and said session key K .

21

22 19. A method according to claim 18 wherein said public information δ is
23 the public key p_A of said first correspondent A.